Issues and Comments about Object Oriented Technology in Aviation

Issue #	Topic	Issue Statement
1	Dead/ deactivated code	Deactivated Code will be found in any application that uses general purposed libraries or object-oriented frameworks. (Note that this is the case where unused code is NOT removed by smart linkers.)
2	Dynamic binding/ dispatch	Flow Analysis, recommended for Levels A-C, is complicated by Dynamic Dispatch (just which method in the inheritance hierarchy is going to be called?).
3	Dynamic binding/ dispatch	Timing Analysis, recommended for Levels A-D is complicated by Dynamic Dispatch (just how much time will be expended determining which method to call?).
4	Dynamic binding/ dispatch	Requirements Testing, recommended for Levels A-D, and Structural Coverage Analysis, recommended for Levels A-C, are complicated by Inheritance, Overriding and Dynamic Dispatch (just how much of the existing verification of the parent class can be reused in its subclasses?).
5	Dynamic binding/ dispatch	Structural Coverage Analysis, recommended for Levels A-C, is complicated by Dynamic Dispatch (just which method in the inheritance hierarchy does the execution apply to?).
6	Dynamic binding/ dispatch	Conformance to the guidelines in DO-178B concerning traceability from source code to object code for Level A software is complicated by Dynamic Dispatch (how is a dynamically dispatched call represented in the object code?).
7	Dynamic binding/ dispatch	Polymorphic, dynamically bound messages can result in code that is error prone and hard to understand.
8	Dynamic binding/ dispatch	Dynamic dispatch presents a problem with regard to the traceability of source code to object code that requires "additional verification" for level A systems as dictated by DO-178B section 6.4.4.2b.
9	Dynamic binding/ dispatch	Dynamic dispatch complicates flow analysis, symbolic analysis, and structural coverage analysis.
10	Dynamic binding/ dispatch	Inheritance, polymorphism, and linkage can lead to ambiguity.

11	Dynamic binding/ dispatch	The use of inheritance and polymorphism may cause difficulties in obtaining structural coverage, particularly decision coverage and MC/DC
12	Dynamic binding/ dispatch	Source to object code correspondence will vary between compilers for inheritance and polymorphism.
13	Dynamic binding/ dispatch	Polymorphic and overloaded functions may make tracing and verifying the code difficult.
14	Inheritance	Requirements Testing, recommended for Levels A-D, and Structural Coverage Analysis, recommended for Levels A-C, are complicated by Inheritance, Overriding and Dynamic Dispatch (just how much of the existing verification of the parent class can be reused in its subclasses?).
15	Inheritance	Multiple interface inheritance can introduce cases in which the developer's intent is ambiguous. (when the same definition is inherited from more than one source is it intended to represent the same operation or a different one?)
16	Inheritance	Flow Analysis and Structural Coverage Analysis, recommended for Levels A-C, are complicated by Multiple Implementation Inheritance (just which of the inherited implementations of a method is going to be called and which of the inherited implementations of an attribute is going to be referenced?). The situation is complicated by the fact that inherited elements may reference one another and interact in subtle ways which directly affect the behavior of the resulting system.
17	Inheritance	Use of inheritance (either single or multiple) raises issues of compatibility between classes and subclasses.
18	Inheritance	Inheritance and overriding raise a number of issues with respect to testing: "Should you retest inherited methods? Can you reuse superclass tests for inherited and overridden methods? To what extent should you exercise interaction among methods of all superclasses and of the subclass under test?"
19	Inheritance	Inheritance can introduce problems related to initialization. "Deep class hierarchies [in particular] can lead to initialization bugs." There is also a risk that a subclass method will be called (via dynamic dispatch) by a higher level constructor before the attributes associated with the subclass have been initialized.

20	Inheritance	"A subclass-specific implementation of a superclass method is [accidentally] omitted. As a result, that superclass method might be incorrectly bound to a subclass object, and a state could result that was valid for the superclass but invalid for the subclass owing to a stronger subclass invariant. For example, Object-level methods like isEqual or copy are not overridden with a necessary subclass implementation".
21	Inheritance	"A subclass [may be] incorrectly located in a hierarchy. For example, a developer locates SquareWindow as a subclass of RectangularWindow, reasoning that a square is a special case of a rectangle ... Suppose that [the method] resize(x, y) is inherited by SquareWindow. It allows different lengths for adjacent sides, which causes SquareWindow to fail after it has been resized. This situation is a design problem: a square is not a kind of a rectangle, or vice versa. Instead both are kinds of four-sided polygons. The corresponding design solution is a superclass FourSidedWindow, of which RectangularWindow and SquareWindow are subclasses."
22	Inheritance	"A subclass either does not accept all messages that the superclass accepts or leaves the object in a state that is illegal in the superclass. This situation can occur in a hierarchy that should implement a subtype relationship that conforms to the Liskov substitution principle."
23	Inheritance	"A subclass computes values that are not consistent with the superclass invariant or superclass state invariants."
24	Inheritance	"Top-heavy multiple inheritance and very deep hierarchies (six or more subclasses) are error-prone, even when they conform to good design practice. The wrong variable type, variable, or method may be inherited, for example, due to confusion about a multiple inheritance structure"
25	Inheritance	The ability of a subclass to directly reference inherited attributes tightly couples the definitions of the two classes.
26	Inheritance	Inheritance can be abused by using it as a "kind of code-sharing macro to support hacks without regard to the resulting semantics"
27	Inheritance	When the same operation is inherited by an interface via more than one path through the interface hierarchy (repeated

		inheritance), it may be unclear whether this should result in a single operation in the subinterface, or in multiple operations.
28	Inheritance	When a subinterface inherits different definitions of the same operation [as a result of redefinition along separate paths], it may be unclear whether/how they should be combined in the resulting subinterface.
29	Inheritance	Use of multiple inheritance can lead to “name clashes” when more than one parent *independently* defines an operation with the same signature.
30	Inheritance	When *different* parent interfaces define operations with different names but compatible specifications, it is unclear whether it should be possible to merge them in a subinterface.
31	Inheritance	It is unclear whether the normal overload resolution rules should apply between operations inherited from different superinterfaces or whether they should not (as in C++).
32	Inheritance	It is important that the overriding of one operation by another and the joining of operations inherited from different sources always be intentional rather than accidental.
33	Inheritance	Multiple inheritance complicates the class hierarchy
34	Inheritance	Multiple inheritance complicates configuration control
35	Inheritance	When inheritance is used in the design, special care must be taken to maintain traceability. This is particularly a concern if multiple inheritance is used.
36	Inheritance	Source to object code correspondence will vary between compilers for inheritance and polymorphism.
37	Inheritance	Overuse of inheritance, particularly multiple inheritance, can lead to unintended connections among classes, which could lead to difficulty in meeting the DO-178B/ED-12B objective of data and control coupling.
38	Inheritance	Multiple inheritance should be avoided in safety critical, certified systems.
39	Inheritance	“Top-heavy multiple inheritance and very deep hierarchies (six or more subclasses) are error-prone, even when they conform to good design practice. The wrong variable type, variable, or method may be inherited, for example, due to confusion about a multiple inheritance structure”

40	Inheritance	Reliance on programmer specified optimizations of the inheritance hierarchy (invasive inheritance) is potentially error prone and unsuitable for safety critical applications.
41	Inheritance	Inheritance, polymorphism, and linkage can lead to ambiguity.
42	Inheritance	Inheritance allows different objects to be treated in the same general way. Inheritance as used in Object Oriented Technology is combining several like things into a fundamental building block. The programmer is allowed to take a group of these like things and refer to them in a general way. One routine can be used for all types that inherit from the fundamental building block. The more often a programmer can use the generic behavior of the parent, the more productive the programmer is. The problem I see is that the generic behavior will not always be precise enough for all the applications, and that critical judgement is required to determine when the programmer needs to specialize the behavior of one of the object rather than use the generic. Who will issue that critical judgement? Who will find all the instances where the general case is too far away from the precision required?
43	Inlining	Flow Analysis, recommended for levels A-C, is impacted by Inlining (just what are the data coupling and control coupling relationships in the executable code?). The data coupling and control coupling relationships can transfer from the inlined component to the inlining component.
44	Inlining	Stack Usage and Timing Analysis, recommended for levels A-D, are impacted by Inlining (just what are the stack usage and worst-case timing relationships in the executable code?). Since inline expansion can eliminate parameter passing, this can effect the amount of information pushed on the stack as well as the total amount of code generated. This, in turn, can effect the stack usage and the timing analysis.
45	Inlining	Structural Coverage Analysis, recommended for levels A-C, is complicated by Inlining (just what is the “logical” coverage of the inline expansions on the original source code?). This is generally only a problem when inlined code is optimized. If statements are removed from the inlined version of a component, then coverage

		of the inlined component is no longer sufficient to assert coverage of the original source code.
46	Inlining	Conformance to the guidelines in DO-178B concerning traceability from source code to object code for Level A software is complicated by Inlining (is the object code traceable to the source code at all points of inlining/expansion?). Inline expansion may not be handled identically at different points of expansion. This can be especially true when inlined code is optimized.
47	Inlining	Inlining may affect tool usage and make structural coverage more difficult for levels A, B, and C.
48	Structural coverage	The unrestricted use of certain object-oriented features may impact our ability to meet the structural coverage criteria of DO-178B.
49	Structural coverage	Statement coverage when polymorphism, encapsulation or inheritance is used.
50	Templates	Templates are instantiated by substituting a specific type argument for each formal type parameter defined in the template class or operation. Passing a test suit for some but not all instantiations cannot guarantee that an untested instantiation is bug free.
51	Templates	Nested templates, child packages (Ada), and friend classes (C++) can result in complex code and hard to read error messages on many compilers.
52	Templates	Templates can be compiled using "code sharing" or "macro-expansion". Code sharing is highly parametric, with small changes in actual parameters resulting in dramatic differences in performance. Code coverage, therefore, is difficult and mappings from a generic unit to object code can be complex when the compiler uses the "code sharing" approach.
53	Templates	Macro-expansion can result in memory and timing issues, similar to those identified for inlining.
54	Templates	The use of templates can result in code bloat. Many C++ compilers cause object code to be repeated for each instance of a template of the same type.
55	Tools	How can we meet the structural coverage requirements of DO-178B with respect to dynamic dispatch? There is cause for

		concern because many current Structural Coverage Analysis tools do not "understand" dynamic dispatch, i.e. do not treat it as equivalent to a call to a dispatch routine containing a case statement that selects between alternative methods based on the run-time type of the object.
56	Tools	How can we meet the control and data flow analysis requirements of DO-178B with respect to dynamic dispatch?
57	Tools	How can deactivated code be removed from an application when general purpose libraries and object-oriented frameworks are used but not all of the methods and attributes of the classes are needed by a particular application?
58	Tools	How can we enforce the rules that restrict the use of specific OO features?
59	Other	Implicit type conversion raises certification issues related to source to object code traceability, the potential loss of data or precision, and the ability to perform various forms of analysis called for by [DO-178B] including structural coverage analysis and data and control flow analysis. It may also introduce significant hidden overheads that affect the performance and timing of the application.
60	Other	Overloading can be confusing and contribute to human error when it introduces methods that have the same name but different semantics. Overloading can also complicate matters for tools (e.g., structural coverage and control flow analysis tools) if the overloading rules for the language are overly complex.
61	Other	Loss of traceability due to the translation of functional requirements to an object-oriented design.
62	Other	Functional coverage of the low level requirement
63	Other	Philosophy of Functional Software Engineering - Most of the training, tools and principles associated with software engineering and assurance, including those of RTCA DO-178B, have been focused on a software function perspective, in that there is an emphasis on software requirements and design and verification of those requirements and the resulting design using reviews, analyses, and requirements-based (functional) testing, and RBT coverage and structural coverage analysis.

		Philosophy of Objects and Operations - Although generally loosely and inconsistently defined, OOT focuses on "objects" and the "operations" performed by and/or to those objects, and may have a philosophy and perspective that are not very conducive to providing equivalent levels of design assurance as the current "functional" approach.
64	Other	Software/software integration testing is often avoided. The position defended by the industry is that the high level of interaction between a great number of objects could lead to a combinative explosion of test cases.
65	Other	Could there be security concerns related to the use of COTS based OOT solutions? Particularly with respect to field loadable software, security risks have been mitigated by the unique architectures of most current systems.
66	Other	Use of dynamic memory allocation/deallocation and use of exception handling were raised as issues by Leanna Rierson in her paper "Object-Oriented Technology (OOT) in Civil Aviation Projects: Certification Concerns" but are currently missing from the list of concerns. If the FAA is concerned about these two items, they should be discussed at the workshop.
67	Other	Most OO languages use reference semantics for passing objects (e.g. Java only supports reference semantics; C++ also supports passing by value but this is rarely used and cannot be used when dynamic binding is required). This results in variables being aliased to each other. It is difficult to analyse the effect of this aliasing on program behaviour because many tools do not allow for the possible presence of aliasing. it is also easy for a developer to inadvertantly use a shallow copy or equality operation where the required semantics can only be achieved by a deep copy or equality operation.
68	Dynamic binding/dispatch	The selection of the code to implement an operation may depend upon more than just the run time type of the target object. In cases involving binary mathematical operations, for instance, this choice typically depends on the run time types of both arguments. As explained in [Bruce et al.], [Castagna] and [MultiJava], this (and other related situations) are not handled

		well by most current OO languages. (A.k.a. "Binary methods problem") References: [Bruce eta al.] Bruce, Kim, Luca Cardelli, Giuseppe Castagna, The Hopkins Object Group, Gary T. Leavens and Benjamin Pierce. On Binary Methods, Iowa State University, technical report #95-08a, December 1995. [Castagna] Castagna, Giuseppe. Object-Oriented Programming: A Unified Foundation, Birkauser, Boston, ISBN: 0-8176-3905-5, 1997. [MultiJava] Clifton, Curtis, Gary T. Leavens, Craig Chambers, and Todd Millstein. "MultiJava: Modular Open Classes and Symmetric Multiple Dispatch for Java", OOPSLA 2000 Conference Proceedings: ACM SIGPLAN Notices, vol. 35, no. 10, October 2000, pp. 130-145.
69	Control flow in OO designs/programs	The use of OO methods typically leads to the creation of many small methods which are physically distributed over a large number of classes. This, and the use of dynamic dispatch, can make it difficult for developers to trace critical paths through the application during design and coding reviews. **JUSTIFICATION**: It is important to be able to specify and review the behavior of the system with respect to scenarios that affect system safety. **PROPOSED SOLUTION**: This issue can be addressed as follows:: 1) At a modeling level, we can use UML sequence diagrams to specify safety critical scenarios during analysis, and refine these during design (by presenting the steps in the scenario at a greater level of detail). Code can then be generated from the overall UML model and reviewed to ensure it complies with the design level sequence diagram (assuming the tool responsible for code generation is not qualified). The analysis and design level scenarios can be developed as a part of a system level safety

		assessment, e.g. as system level scenarios that could lead to hazards. 2) At a source code level, we can use aspects to physically group the methods called in such scenarios, so that they appear in a single file. Note: Although the methods definitions are physically grouped in this way in order to create the source code equivalent of an analysis or design scenario, they are still associated with different classes in accordance with the OO principles of encapsulation and data abstraction. 3) Both 1 and 2, with the generation of aspects from UML models. **RELATED TOPICS**: Dynamic dispatch, traceability (of analysis to design to code)
70	Traceability	The difference between dead and deactivated code is not always clear when using OOT. Without good traceability, identifying dead vs. deactivated code may be difficult or impossible.
71	Traceability	When a design contains abstract base classes, portions of the implementations of these classes may be overridden in more specialized subclasses, resulting deactivated code.
72	Traceability	Traceability is made more difficult because there is often a lack of OO methods or tools for the full software lifecycle.
73	Other	Formal specification languages are generally accessible only to those specially trained to use them. To make formal specifications accessible to developers and the authors of test cases, we must map such formal specifications to natural language and/or other less formal notations (e.g. UML). There, however, is currently no well defined means of doing so. This issue applies to both preliminary and detailed design.
74	Other	Change impact analysis may be difficult or impossible due to difficulty in tracing functional requirements through implementation.
75	Other	Limitations of UML may limit how non-functional and cross-cutting requirements of realtime, safety critical, distributed, fault-tolerant, embedded systems are captured in UML and traced to the design, implementation, and test cases.

76	Other	Configuration management may be difficult in OO systems, causing traceability problems. If the objects and classes are considered configuration items, they can be difficult to trace, when used multiple times in slightly different manners.
77	Traceability	What is "low level requirements" for OO? Affects how we do low-level testing. If we don't know what low-level requirements are, we don't know the appropriate level of testing. * High level = WHAT * Low level = HOW Related to issue raised in tools session – relation be between artifacts. Should be addressed in the handbook.
78	Traceability	Addressing derived requirements for OO – how does this happen? How is it different than traditional and how does it tie up to the safety assessment.Not really unique for OO. Will be addressed when we do the artifact mapping.
79	Traceability	Difficult to identify individual atomic requirements in OO. UML tends to group requirements in a graphical format. Would complicate matters if considered derived. For derived requirements, the entire graph would be passed to the safety folk for evaluation of safety impact.
80	Traceability	Lower levels of decomposition may not be possible for some requirements (e.g., performance requirements). Levels of abstraction may be different than traditional.
81	Traceability	Are there unique challenges for source to object code traceability in non-Level A systems? Where should this be addressed? Multiple tools and ways of addressing s-to-o traceability? (not really new) Beyond what DO-178B requires. More of a "DO-178C" issue. Out of scope for the handbook. Is UML the "source code" for OO?

82	Traceability	Is there another "class" of tool qualification for visual modeling tools to demonstrate the integrity of these tools? Not necessarily automating a step, but are looking to make sure the tool is doing what you want. How to ensure consistency of the tools (validating the tool)? How to validate the tool when changes occur? Typically part of the tool selection process. Concern seems to be addressed by handbook mod.
83	Traceability	Auto-test and code generation tools – what are the concerns when a single tool generates code and test from the same model? The concern is with the independence – same input and same tool. Already covered by DO-178B. Not necessarily OO-specific, but may be more prevalent with OO tools. Need to be addressed in some other document or forum.
84	Traceability	Maintaining tool environment, archives, … when licenses are involved is not clear. May need to have some kind of "permanent license" to support safety and continued airworthiness of the aircraft. OO more dependent on tools, but not necessarily an OO-specific issue.
85	Traceability	Maturity/long-term support of tools. Tool manufacturers may not realize the long-life need of tools. Is this a higher risk in the OO environment? Education for both the tool and aviation communities to understand the specific needs for tool manufacturers and aircraft manufacturers. Not necessarily OO-specific, but might be more prevalent with OO.
86	Traceability	Are there other types of OO tools that need to be addressed? Need to anticipate other classes of tools that may come onto the scene. E.g., traceability tool for OO, transformation tools, CM tools, refactoring tools (tool to restructure source code to meet new requirements),
87	Traceability	How does OO life cycle data map to the DO-178B section 11 life cycle data? E.g., What "source code" mean in OO? What is req, design, code? Transition from text-based to model-based artifacts.

		*** May need to clarify this up front in the handbook, when making the tie between DO-178B and the handbook.
88	Traceability	Configuration management and incremental development of OO projects and tools. When CM comes into play during the development process may be different than our current practices, when using an UML tool. Doing more iterations in OO. How to "get credit" on iterations. Not necessarily OO-specific, but might be more prevalent with OO because of the multiple iterations.
89	Traceability	Is dynamic dispatch compatible with DO-178B required forms of static analysis? Mention that dynamic dispatch hinders some forms of static analysis including (see DO-178B section 6.3.4f). Tools can treat this if complete closure exists. DO-178B requires complete closure. In cases of incomplete closure, need to define ways to implement.
90	Traceability	Fundamental pre-requisite language issues need clarification prior to adopting LSP and DBC. How can LSP be implemented using available languages? Strongly consider a language subset that is amenable to use of LSP and DBC. Concern is how far to take this subset.
91	Dynamic binding/ dispatch	Inconsistent Type Use (ITU): When a descendant class does not override any inherited method (i.e., no polymorphic behavior), anomalous behavior can occur if the descendant class has extension methods resulting in an inconsistent inherited state.
92	Dynamic binding/ dispatch	State Definition Anomaly (SDA): If refining methods do not provide definitions for inherited state variables that are consistent with definitions in an overridden method, a data flow anomaly can occur.
93	Dynamic binding/ dispatch	State Definition Inconsistency (SDIH): If an indiscriminately-named local state variable is introduced, a data flow anomaly can result.
94	Dynamic binding/ dispatch	State Defined Incorrectly (SDI): If a computation performed by an overriding method is not semantically equivalent to the computation of the overridden method wrt a variable, a behavior anomaly can result.

95	Dynamic binding/ dispatch	Indirect Inconsistent State Definition (IISD): When a descendent adds an extension method that defines an inherited state variable, an inconsistent state definition can occur.
96	Dynamic binding/ dispatch	Anomalous construction behavior (ACB1): If a descendant class provides an overriding definition of a method which uses variables defined in the descendant's state space, a data flow anomaly can occur.
97	Dynamic binding/ dispatch	Anomalous construction behavior (ACB2): If a descendant class provides an overriding definition of a method which uses variables defined in the ancestor's state space, a data flow anomaly can occur.
98	Dynamic binding/ dispatch	Incomplete construction (IC): If the constructor does not establish initial state conditions and the state invariants for new instances of a class, then a state variable may have in incorrect initial value or a state variable may not have been initialized.
99	Dynamic binding/ dispatch	State Visibility Anomaly (SVA): When private state variables exist, if every overriding method in a descendant class doesn't call the overridden method in the ancestor class, a data flow anomaly can exist.